

Patent Claims

1. A method for checking the authenticity of a manager application (50...100) in a telecommunications management network operating system TMN-OS by means of a network element which is managed by the TMN-OS via an intermediate TMN, having the following steps:
- transmission of communication-protocol-specific authentication data from a manager application (50, 60...100) via the TMN to the network element in the course of handling a communication protocol, in which case the protocol-specific authentication data are required for the network element to check the authenticity of the manager application (50, 60...100); and
- checking the authenticity of the manager application by comparison of the received protocol-specific authentication data with predetermined, stored authentication data;
- characterized in that
- the step of authentication checking is carried out centrally in an authenticity checking device (20) for various communication protocols; and in that
- authentication data for all the communication protocols used are stored centrally in an authentication databank (10).
2. The method as claimed in claim 1, furthermore characterized by the following step:

management of the central authentication databank (10) by means of a dedicated communication protocol.

5 3. The method as claimed in claim 1 or 2, characterized in that the communication protocols are a Q3, FTAM, FTP or MML protocol.

10 4. The method as claimed in one of claims 1 to 3, characterized in that the step of authentication checking for each individual communication protocol is carried out centrally in the authenticity checking device using different authentication types.

15 5. A network element in a telecommunications network, in which case the network element is managed by a telecommunications management network operating system TMN-OS via a telecommunications management network TMN, having:

20

at least one agent application (55, 65...105) for receiving communication-protocol-specific authentication data via the TMN from an associated manager application (50, 60...100) in the TMN-OS, in which case the authentication data are required for checking the authenticity of the associated manager application; and

25

30 an authenticity checking device (20), for receiving the protocol-specific authentication data from the agent application and for checking the authenticity of the management application by comparison of the protocol-specific authentication data with predetermined, stored authentication data;

35

characterized in that

the authenticity checking device (20) carries out the authentication checking centrally for various communication protocols, and in that

5 the authentication data for all the communication protocols used are stored centrally in an authentication databank (10).

10 6. The network element as claimed in claim 5, characterized in that said network element also has a management device (30) which manages the central authentication databank (10).

15 7. The network element as claimed in claim 6, characterized in that the management device (30) is coupled to the TMN via a dedicated agent application (105) and is controlled by the TMN-OS.

09936926-091904